Counting points on (more general) curves

Jan Tuitman, KU Leuven

November 14, 2013
Zeta functions

Suppose that
- $F_q$ finite field of cardinality $q = p^n$.
- $X/F_q$ a smooth proper algebraic curve of genus $g$.

Recall that the zeta function of $X$ is defined as

$$Z(X, T) = \exp\left(\sum_{i=1}^{\infty} |X(F_{q^i})| \frac{T^i}{i}\right).$$

It follows from the Weil conjectures that $Z(X, T)$ is of the form

$$\frac{\chi(T)}{(1 - T)(1 - qT)},$$

where $\chi(T) \in Z[T]$ of degree $2g$, with inverse roots that
- have absolute value $q^{1/2}$
- are permuted by the map $x \to q/x$. 
Computing zeta functions

Problem

*How to compute* $Z(X, T)$ *(efficiently)*?

Note that this problem has cryptographic applications when $X$ is a (hyper)elliptic curve.

Theorem

Let $F_p$ denote the $p$th power Frobenius map and $H^*_{\text{rig}}(X)$ the rigid cohomology. Then

$$
\chi(T) = \det(1 - T F_p^n | H^1_{\text{rig}}(X)).
$$
Suppose that $p \neq 2$. A hyperelliptic curve $X$ is given by an (affine) equation of the form

$$y^2 = Q(x),$$

with $Q \in \mathbb{F}_q[x]$ a monic polynomial of degree $2g + 1$ with $\gcd(Q, Q') = 1$.

To define $H^{1}_{\text{rig}}(X)$, we start by lifting $Q$ to characteristic 0:

Let $Q \in \mathbb{Z}_q[x]$ denote a monic lift of $Q$ of degree $2g + 1$. 


Some rings

We define a ring \( \mathbb{Z}_q \langle x, y, y^{-1} \rangle^\dagger \) of overconvergent functions:

\[
\left\{ \sum_{i=0}^{\infty} \sum_{j=-\infty}^{\infty} a_{i,j} x^i y^j \mid a_{i,j} \in \mathbb{Z}_q, \exists \rho > 1: \lim_{i+|j| \to \infty} |a_{i,j}| \rho^i = 0 \right\}.
\]

Moreover, we denote

\[
\mathcal{R} = \mathbb{Z}_q[x, y, y^{-1}]/(Q), \quad \mathcal{R}^\dagger = \mathbb{Z}_q \langle x, y, y^{-1} \rangle^\dagger/(Q)
\]

\[
\mathcal{U} = \text{Spec} \mathcal{R}, \quad \mathcal{U} = \mathcal{U} \otimes \mathbb{Q}_q, \quad \mathcal{U} = \mathcal{U} \otimes \mathbb{F}_q.
\]
Rigid cohomology

We define the overconvergent Kähler differentials

$$\Omega^1_{R^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{(2ydy - Q' dx)}$$

and the overconvergent De Rham complex

$$\Omega_{R^\dagger}^\bullet : 0 \longrightarrow R^\dagger \overset{d}{\longrightarrow} \Omega_{R^\dagger} \longrightarrow 0.$$

We then have

$$H^1_{\text{rig}}(U) = H^1(\Omega_{R^\dagger}^\bullet \otimes \mathbb{Q}_q) = \text{coker}(d) \otimes \mathbb{Q}_q.$$
The $p$th power Frobenius map on $\mathcal{R} \otimes F_q$ can be lifted to $\mathcal{R}$.

If $\sigma \in \text{Gal}(Q_q/Q_p)$ denotes the unique lift of the $p$th power Frobenius map on $F_q$, then

$$F_p(y)^2 = Q^\sigma(F_p(x)).$$

So we define

$$F_p(x) = x^p,$$

$$F_p(y) = Q^\sigma(x^p)^{\frac{1}{2}} = y^p \left(1 + \frac{Q^\sigma(x^p) - Q(x)^p}{y^{2p}}\right)^{\frac{1}{2}}.$$ 

The square root can be computed efficiently by Hensel lifting.
Computing in the cohomology

We can write any 1-form $\omega \in \Omega^1_R$ as

$$\sum_{i=-\infty}^{\infty} a_i(x) \frac{dx}{y^i},$$

with $a_i \in \mathbb{Z}_q[x]$ of degree $< 2g + 1$ for all $i \in \mathbb{Z}$. Writing $B(x) = A_1(x)Q(x) + A_2(x)Q'(x)$, we have

$$B(x) \frac{dx}{y^i} \equiv \left( A_1(x) + \frac{2A_2'(x)}{i-2} \right) \frac{dx}{y^{i-2}}.$$

This allows us to eliminate all terms with $i > 2$. We can do something similar for the terms with $i \leq 0$. 
A basis for the cohomology

As a consequence, one can show that:

**Theorem**

A basis for $H^1_{\text{rig}}(U)$ is given by

$$[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}, x^0 \frac{dx}{y^2}, \ldots, x^{2g} \frac{dx}{y^2}]$$

and the first $2g$ vectors form a basis for the subspace $H^1_{\text{rig}}(X)$. 
A rough sketch:

- Compute $F_p\left(\frac{1}{y}\right)$ and $F_p\left(x^i \frac{dx}{y}\right) = px^{ip+p-1}F_p\left(\frac{1}{y}\right)dx$.
- Reduce back to the basis $[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}]$ and read off the matrix $A$ of $F_p$ on $H^1_{\text{rig}}(X)$.
- Compute the matrix $A^{(n)} = A^{\sigma^{n-1}} \ldots A^\sigma$ of $F_p^n$ on $H^1_{\text{rig}}(X)$.
- Determine $\chi(T) = \det(1 - F_p^n T|H^1_{\text{rig}}(X))$.

The polynomial $\chi(T) = \sum_{i=0}^{2g} \chi_i T^i \in \mathbb{Z}[T]$ is determined exactly if known to high enough $p$-adic precision, since there are explicit bounds for the size of its coefficients.
More general curves

We let $X/F_q$ denote the smooth projective curve given by the (affine) equation

$$Q(x, y) = y^d + Q_{d-1}(x)y^{d-1} + \ldots + Q_0 = 0,$$

where $Q(x, y)$ is irreducible separable and $Q_i(x) \in F_q[x]$ for all $0 \leq i \leq d - 1$.

We let $Q \in \mathbb{Z}_q[x]$ denote a lift of $Q$ that is monic of degree $d$ in $y$.

**Proposition**

The $\mathbb{Z}_q[x]$-module $\mathbb{Z}_q[x, y]/(Q)$ is free with basis $[1, y, \ldots, y^{d-1}]$. 
Some notation

Definition

We let $\Delta(x) \in \mathbb{Z}_q[x]$ denote the resultant of $Q$ and $\frac{\partial Q}{\partial y}$ with respect to the variable $y$ and $r(x) \in \mathbb{Z}_q[x]$ the squarefree polynomial $r = \Delta/(\gcd(\Delta, \frac{d\Delta}{dx}))$.

Note that $\Delta(x) \neq 0 \pmod{p}$ since the map $x$ is separable.

Definition

$S = \mathbb{Z}_q[x, \frac{1}{r}]$, \hspace{1cm} R = \mathbb{Z}_q[x, \frac{1}{r}, y]/(Q)$,

$S^\dagger = \mathbb{Z}_q\langle x, \frac{1}{r} \rangle^\dagger$, \hspace{1cm} R^\dagger = \mathbb{Z}_q\langle x, \frac{1}{r}, y \rangle^\dagger/(Q)$,

and write $\mathcal{V} = \text{Spec } S$, $\mathcal{U} = \text{Spec } R$, so that $x$ defines a finite étale morphism from $\mathcal{U}$ to $\mathcal{V}$.
The following assumption is essential:

**Assumption**

1. There exists a smooth proper curve $\mathcal{X}$ over $\mathbb{Z}_q$ and a smooth relative divisor $\mathcal{D}_\mathcal{X}$ on $\mathcal{X}$ such that $\mathcal{U} = \mathcal{X} \setminus \mathcal{D}_\mathcal{X}$. We write $\mathcal{X} = \mathcal{X} \otimes \mathbb{Q}_q$ for the generic fibre of $\mathcal{X}$.

2. There exists a smooth relative divisor $\mathcal{D}_{\mathbb{P}^1}$ on $\mathbb{P}^1_{\mathbb{Z}_q}$ such that $\mathcal{V} = \mathbb{P}^1_{\mathbb{Z}_q} \setminus \mathcal{D}_{\mathbb{P}^1}$.

**Definition**

We let $\mathcal{U} = \mathcal{U} \otimes_{\mathbb{Z}_q} \mathbb{F}_q$, $\mathcal{V} = \mathcal{V} \otimes_{\mathbb{Z}_q} \mathbb{F}_q$ denote the special fibres and $\mathcal{U} = \mathcal{U} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$, $\mathcal{V} = \mathcal{V} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ the generic fibres of $\mathcal{U}$ and $\mathcal{V}$, respectively.
For convenience, we assume:

**Assumption**

*The zero locus of $Q$ in $\mathbb{A}_\mathbb{Z}^2$ is smooth over $\mathbb{Z}_q$.***

**Proposition**

*The element $s = r / \frac{\partial Q}{\partial y}$ of $Q_q(x, y)$ is contained in $\mathbb{Z}_q[x, y]/(Q)$.***

**Sketch of the proof:** $\Delta / \frac{\partial Q}{\partial y}$ is contained in $\mathbb{Z}_q[x, y]/(Q)$ by the definition of $\Delta$ as the determinant of the Sylvester matrix. By the assumption, $[1, y, \ldots, y^{d-1}]$ is an integral basis of $Q_q[x, y]/(Q)$ over $Q_q[x]$. So for any monic irreducible polynomial $\pi \in \mathbb{Z}_q[x]$, the element $\frac{\partial Q}{\partial y} / \pi$ of $Q_q(x, y)$ is not integral at $(\pi)$ because of the term $(d/\pi)y^{d-1}$, hence its inverse $\pi / \frac{\partial Q}{\partial y}$ is integral (even zero) at $(\pi)$. Since $\prod_{\pi | \Delta \pi = r$, this proves the Proposition.
Frobenius lift

Define sequences \((\alpha_i)_{i \geq 0}, (\beta_i)_{i \geq 0}\), with \(\alpha_i \in S^\dagger\) and \(\beta_i \in \mathcal{R}^\dagger\), by the following recursion:

\[
\alpha_0 = \frac{1}{r^p}, \quad \beta_0 = y^p,
\]
\[
\alpha_{i+1} = \alpha_i (2 - \alpha_i r^\sigma(x^p)) \quad \text{(mod } p^{2i+1}),
\]
\[
\beta_{i+1} = \beta_i - Q^\sigma(x^p, \beta_i) s^\sigma(x^p, \beta_i) \alpha_i \quad \text{(mod } p^{2i+1}).
\]

Then one easily checks that the \(\sigma\)-semilinear ringhomomorphism \(F_p : \mathcal{R}^\dagger \to \mathcal{R}^\dagger\) defined by

\[
F_p(x) = x^p, \quad F_p(1r) = \lim_{i \to \infty} \alpha_i, \quad F_p(y) = \lim_{i \to \infty} \beta_i,
\]

is a Frobenius lift.
The connection matrix

**Definition**

Let $M \in M_{d \times d}(\mathbb{Z}_q[x])$ denote the matrix for which

$$d(y^j) = jy^{j-1} dy = -jy^{j-1} s \frac{\partial Q}{\partial x} dx = \sum_{i=0}^{d-1} \left( \frac{M_{ij}}{r} \right) y^i dx,$$

for all $0 \leq j \leq d - 1$ as 1-forms on $\mathcal{U}$.

For convenience, we assume:

**Assumption**

$\deg(M) < \deg(r)$, or equivalently $(M/r) dx$ has at most a simple pole at $x = \infty$. 
The exponents

**Definition**

Let $x_0 \in \mathbb{P}^1(\overline{\mathbb{Q}}_q)$ be a geometric point $\neq \infty$. The exponents of $(M/r)dx$ at $x_0$ are defined as the eigenvalues of the residue matrix $(x - x_0)(M/r)|_{x=x_0}$. Moreover, the exponents of $(M/r)dx$ at $\infty$ are defined as its exponents at $t = 0$, after substituting $x = 1/t$.

**Proposition**

The exponents of $(M/r)dx$ at any point $x_0 \in \mathbb{P}^1(\overline{\mathbb{Q}}_q)$ are elements of $\mathbb{Q} \cap \mathbb{Z}_p$. For $x_0 \neq \infty$ they are contained in the interval $[0, 1)$ and for $x_0 = \infty$ in the interval $[(d - 1)\mu, 0]$, where

$$\mu = \min\left\{ \frac{\text{ord}_P(y)}{e_P} : P \in x^{-1}(\infty) \right\}.$$
Effective convergence bounds

Proposition

Let $N \in \mathbb{N}$. Then modulo $p^N$:

1. $F_p(1/r)$ is congruent to $\sum_{i=p}^{pN} \frac{\rho_i(x)}{r^i}$, where for all $p \leq i \leq pN$ the polynomial $\rho_i \in \mathbb{Z}_q[x]$ satisfies $\deg(\rho_i) < \deg(r)$.

2. $F_p(y^i)$ is congruent to $\sum_{j=0}^{d-1} \phi_{i,j}(x)y^j$, where

\[
\phi_{i,j} = \sum_{k=0}^{p(N-1)+1} \frac{\phi_{i,j,k}(x)}{r^k},
\]

for all $0 \leq i, j \leq d - 1$ and $\phi_{i,j,k} \in \mathbb{Z}_q[x]$ satisfies $\deg(\phi_{i,j,0}) < p(d - 1)(-\mu)$ and $\deg(\phi_{i,j,k}) < \deg(r)$, for all $0 \leq i, j \leq d - 1$ and $1 \leq k \leq p(N - 1) + 1$.

Proposition

For all \( \ell \in \mathbb{N} \) and every vector \( w \in \mathbb{Q}_q[x]^{\oplus d} \), there exist (unique) vectors \( u, v \in \mathbb{Q}_q[x]^{\oplus d} \) with \( \deg(v) < \deg(r) \), such that

\[
\sum_{i=0}^{d-1} \frac{w_i y^i}{r^\ell} \frac{dx}{r} = d \left( \sum_{i=0}^{d-1} \frac{v_i y^i}{r^\ell} \right) + \sum_{i=0}^{d-1} \frac{u_i y^i}{r^{\ell-1}} \frac{dx}{r}
\]

as 1-forms on \( \mathbb{U} \).

Sketch of the proof: \( r \) is separable, so \( r' \) is invertible in \( \mathbb{Q}_q[x]/(r) \). \( v \) has to satisfy \( \left( \frac{M}{r'} - \ell I \right) v \equiv \frac{w}{r'} \pmod{r} \) over \( \mathbb{Q}_q[x]/(r) \). The finite exponents of \( (M/r)dx \) are contained in \([0, 1)\), hence \( \det(\ell I - M/r') \) is invertible in \( \mathbb{Q}_q[x]/(r) \), so there is a unique solution \( v \). We now take

\[
u = \frac{w - \left( M - \ell r' I \right) v}{r} - \frac{dv}{dx}.
\]
Proposition

For every vector \( w \in \mathbb{Q}_q[x]^{\oplus d} \) with \( \deg(w) \geq \deg(r) \), there exist vectors \( u, v \in \mathbb{Q}_q[x]^{\oplus d} \) with \( \deg(u) < \deg(w) \), such that

\[
\frac{\sum_{i=0}^{d-1} w_i y^i}{r} \, dx = d \left( \sum_{i=0}^{d-1} v_i y^i \right) + \left( \sum_{i=0}^{d-1} u_i y^i \right) \frac{dx}{r}
\]

as 1-forms on \( \mathbb{U} \).

Sketch of the proof: We denote \( t = 1/x \). Since \( \deg(M) < \deg(r) \), we can expand

\[
\frac{M}{r} \, dx = \left( \frac{M_{-1}}{t} + M_0 + \ldots \right) \, dt,
\]

where \( M_i \in M_d \times d(\mathbb{Q}_q) \) for all \( i \). Similarly, if \( k = \deg(w) - \deg(r) + 2 \), then we can write

\[
\frac{\sum_{i=0}^{d-1} w_i y^i}{r} \, dx = \left( \frac{b_{-k}}{t^k} + \frac{b_{-(k-1)}}{t^{k-1}} + \ldots \right) \, dt,
\]

where \( b_i \in (\mathbb{Q}_q)^{\oplus d} \) for all \( i \). The infinite exponents of \((M/r)\, dx\) are \( \leq 0 \), so the linear system \((M_{-1} - (k-1)I)c = b_{-k}\) has a unique solution \( c \in (\mathbb{Q}_q)^{\oplus d} \). We now take

\[
v = cx^{k-1} \quad \text{and} \quad u = w - (Mv + r \frac{dv}{dx}).
\]
Theorem

Every class in $H^1_{\text{rig}}(U)$ is represented by a 1-form of the form

$$
\left( \sum_{i=0}^{d-1} u_i(x)y^i \right) \frac{dx}{r},
$$

where $u_i \in \mathbb{Q}_q[x]$ satisfies $\deg(u_i) < \deg(r)$ for all $0 \leq i \leq d - 1$.

Sketch of the proof: By a comparison theorem of Baldassarri and Chiarellotto, we can restrict to classes that lie in $H^1_{dR}(U)$. Using the previous two propositions (both repeatedly), such a class can be reduced to the required form.
Proposition

Let \( \omega \in \Omega^1_\mathcal{U} \) be of the form

\[
\omega = \frac{\sum_{i=0}^{d-1} w_i(x) y^i}{r^\ell} \frac{dx}{r},
\]

where \( \ell \in \mathbb{N} \) and \( w_i \in \mathbb{Z}_q[x] \) satisfies \( \deg(w_i) < \deg(r) \) for all \( 0 \leq i \leq d - 1 \). We define \( e_0 = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) \neq \infty\} \). If we represent the class of \( \omega \) in \( H^1_{\text{rig}}(U) \) as in the Theorem using the Proposition, then

\[
p^{\lfloor \log_p(\ell e_0) \rfloor} u_i(x) \in \mathbb{Z}_q[x]
\]

for all \( 0 \leq i \leq d - 1 \).
Proposition

Let $\omega \in \Omega^1_U$ be of the form

$$\omega = \left( \sum_{i=0}^{d-1} w_i(x)y^i \right) \frac{dx}{r},$$

where $w_i \in \mathbb{Z}_q[x]$ for all $0 \leq i \leq d - 1$ and $\deg(w_i) \geq \deg(r)$ for some $0 \leq i \leq d - 1$. We define $m = (\deg(w) - \deg(r) + 1)$ and $e_\infty = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) = \infty\}$. If we represent the class of $\omega$ in $H^1_{\text{rig}}(U)$ as in the Theorem using the Proposition, then

$$p^{\lfloor \log_p((m-(d-1)\mu)e_\infty) \rfloor} u_i(x) \in \mathbb{Z}_q[x]$$

for all $0 \leq i \leq d - 1$. 
A basis for the cohomology

First, let $E$ denote the $\mathbb{Q}_q$-vector space of 1-forms

$$\omega = \left( \sum_{i=0}^{d-1} u_i(x)y^i \right) \frac{dx}{r},$$

where $u_i \in \mathbb{Q}_q[x]$ satisfies $\deg(u_i) < \deg(r)$ for all $0 \leq i \leq d - 1$. Now, let $E_1$ denote the kernel of the map that sends $\omega \in E$ to the element $\frac{\partial Q}{\partial y} \sum_{i=0}^{d-1} u_i y^i$ of $\mathbb{Q}_q[x, y]/(Q, r)$. Finally, let $E_2$ denote the subspace of $E_1$ generated by the elements $d(y^i)$ for all $0 \leq i \leq d - 1$.

**Theorem**

*We have isomorphisms:*

$$H^1_{\text{rig}}(U) \cong E/E_2, \quad H^1_{\text{rig}}(X - x^{-1}(\infty)) \cong E_1/E_2.$$
Some remarks

- This allows us to compute $Z(X - x^{-1}(\infty), T)$, from which $Z(X, T)$ can be easily obtained.
- All assumptions but the first one can be removed by temporarily changing from $[y^0, \cdots, y^{d-1}]$ to another basis if equations for $X$ are known.
- The way we compute in the cohomology is inspired by work of Lauder (and his student Walker) on the so called fibration method.
An example

Hyperelliptic curve $y^2 = f(x)$ with $f$ of degree $2g + 1$.

$\Delta(x) = r(x) = f(x)$.

$(M/r)dx = \begin{pmatrix} 0 & 0 \\ 0 & \frac{f'(x)}{2f(x)} \end{pmatrix}$

Finite exponents $0, 1/2$ and infinite ones $-(2g + 1)/2, 0$.

$$E = \{(u_0(x) + u_1(x)y)dx/y^2\}$$

$$E_1 = \{u_1(x)ydx/y^2\}$$

$$E_2 = \{f'(x)ydx/y^2\}$$

This gives the same basis for the cohomology as before.